



FEDERAL RETIREMENT THRIFT INVESTMENT BOARD

Privacy Act of 1974; System of Records

AGENCY: Federal Retirement Thrift Investment Board (FRTIB).

ACTION: Notice of Modified System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Federal Retirement Thrift Investment Board (FRTIB) is proposing to modify its system of records for fraud and forgery records. Records contained in this system are used to investigate potential or actual fraud against TSP participant or beneficiary accounts. FRTIB is modifying this system of records to account for its process for addressing new alerts the Financial Services Information Sharing and Analysis Center (FS-ISAC) sends to FRTIB to better help protect and secure participant account information.

DATES: This system will become effective upon its publication in today's Federal Register. FRTIB is not proposing any changes to the routine uses.

ADDRESSES: You may submit written comments to FRTIB by any one of the following methods:

- *Federal eRulemaking Portal:* <https://www.regulations.gov>. Follow the website instructions for submitting comments.
- *Fax:* (202) 942-1676.
- *Mail or Hand Delivery:* Office of General Counsel, Federal Retirement Thrift Investment Board, 77 K Street NE, Suite 1000, Washington, DC 20002.

FOR FURTHER INFORMATION CONTACT: Marla Greenberg, Chief Privacy Officer, Federal Retirement Thrift Investment Board, Office of General Counsel, 77 K Street NE, Suite 1000, Washington, DC 20002, (202) 942-1600. For access to any of the FRTIB's system of records, contact Amanda Haas, FOIA Officer, Office of General Counsel, at the above address and phone number.

SUPPLEMENTARY INFORMATION: FRTIB is proposing to modify its system of records for fraud and forgery records, entitled, "FRTIB-13, Fraud and Forgery Records." The proposed changes are necessary because they enable the FRTIB to protect participant accounts based on additional information FRTIB receives from the FS-ISAC, concerning account credentials that may have been compromised. FRTIB is proposing to amend the purpose of the system of records to provide additional context around how the Agency protects participant accounts from fraudulent activity. FRTIB is proposing to change the categories of individuals covered by the system, to include information about participants and beneficiaries who may be actual or potential victims of fraud.

Additionally, FRTIB is proposing to modify the category of records in the system to include telephone numbers, IP addresses, and notifications from FS-ISAC, which includes potentially or actually compromised credentials participants use to log into their TSP account online. FRTIB is

also proposing a change to record source categories to include FS-ISAC. Finally, FRTIB is proposing technical and clarifying language to conform to the standards established in OMB Circular A-108, but these changes are not substantive in nature. FRTIB is not proposing modifications to its routine uses or exemptions claimed.

Megan Grumbine,
General Counsel and Senior Agency Official for Privacy

SYSTEM NAME: Fraud and Forgery Records.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are located at the Federal Retirement Thrift Investment Board, 77 K Street NE, Suite 1000, Washington, DC 20002. Records may also be kept at an additional location for Business Continuity purposes.

SYSTEM MANAGER: Supervisory Fraud Specialist, Federal Retirement Thrift Investment Board, 77 K Street NE, Suite 1000, Washington, DC 20002.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 8474; and 44 U.S.C. 3101.

PURPOSE(S): These records are used to inquire into and investigate allegations that a TSP participant, beneficiary, alternate payee, or third party has committed or attempted to commit an act of fraud or forgery relating to a participant or beneficiary account or the Thrift Savings Fund; *to prevent fraud and to protect participant accounts from potential fraud*; and to collect information to verify allegations that a third party has misappropriated the FRTIB's (or TSP's) name, brand, or logos.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: This system of records contains information on Thrift Savings Plan (TSP) participants, beneficiaries, alternate payees, and third party individuals alleged to have committed an act of fraud or forgery relating to participant and beneficiary accounts; and third parties alleged to have misappropriated, or attempted to misappropriate the FRTIB's (including the TSP's) name, brand, or logos. *This system of records also contains information about TSP participants and beneficiaries who may be actual or potential victims of fraud.*

CATEGORIES OF RECORDS IN THE SYSTEM: These records contain the following kinds of information: name, date of birth, *telephone number, IP address*, and Social Security number of TSP participants, beneficiaries, alternate payees, and third parties alleged to have committed an act of fraud or forgery relating to participant accounts or the Thrift Savings Fund; TSP account information related to the fraud or forgery allegation; information obtained from other agencies as it relates to allegations of fraud or forgery; documentation of complaints and allegations of fraud and forgery; exhibits, statements, affidavits, or records obtained during investigations of fraud, or forgery, court and administrative orders, transcripts, and documents; internal staff memoranda; staff working papers; *notifications from the Financial Services*

Information Sharing and Analysis Center (FS-ISAC), including credentials used to log into MyAccount that have been potentially or actually compromised; and other documents and records related to the investigation of fraud or forgery, including the disposition of the allegations; and reports on the investigation.

RECORD SOURCE CATEGORIES: Records in this system may be provided by or obtained from the following: persons to whom the information relates when practicable, including TSP participants, beneficiaries, alternate payees, or other third parties; complainants; informants; witnesses; investigators; persons reviewing the allegations; Federal, state and local agencies; *FS-ISAC*; and investigative reports and records.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, as amended, 5 U.S.C. 552a(b); and:

1. A record from this system may be disclosed to the Federal Bureau of Investigation; Department of Justice; Securities and Exchange Commission; Federal Trade Commission; Consumer Financial Protection Bureau; or the Financial Industry Regulatory Authority for further investigation, prosecution, or enforcement.
2. A record from this system may be disclosed to the Secret Service for the purpose of investigating forgery, and to the Department of Justice, when substantiated by the Secret Service.
3. A record pertaining to this system may be disclosed to the current or former employing agency of the participant, beneficiary, alternate payee, or third party alleged to have committed fraud or forgery against a participant account or the Thrift Savings Fund for the purpose of further investigation or administrative action.
4. A record from this system may be disclosed to informants, complainants, or victims to the extent necessary to provide those persons with information and explanations concerning the progress or results of the investigation.
5. Audit: A record from this system of records may be disclosed to an agency, organization, or individual for the purpose of performing an audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FRTIB officers and employees.
6. Breach Mitigation and Notification: Response to Breach of FRTIB Records: A record from this system of records may be disclosed to appropriate agencies, entities, and

persons when (1) FRTIB suspects or has confirmed that there has been a breach of the system of records; (2) FRTIB has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, FRTIB (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with FRTIB's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

7. Response to Breach of Other Records: A record from this system of records may be disclosed to another Federal agency or Federal entity, when FRTIB determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
8. Congressional Inquiries: A record from this system of records may be disclosed to a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains.
9. Contractors, et al.: A record from this system of records may be disclosed to contractors, grantees, experts, consultants, the agents thereof, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for FRTIB, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FRTIB officers and employees.
10. Investigations, Third Parties: A record from this system of records may be disclosed to third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the third party officer making the disclosure.
11. Investigations, Other Agencies: A record from this system of records may be disclosed to appropriate Federal, state, local, tribal, or foreign government agencies or multilateral governmental organizations for the purpose of investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where FRTIB determines that the information would assist in the enforcement of civil or criminal laws.
12. Law Enforcement Intelligence: A record from this system of records may be disclosed to a Federal, state, tribal, local, or foreign government agency or organization, or

international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

13. Law Enforcement Referrals: A record from this system of records may be disclosed to an appropriate Federal, state, tribal, local, international, or foreign agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.
14. Litigation, DOJ or Outside Counsel: A record from this system of records may be disclosed to the Department of Justice, FRTIB's outside counsel, other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (1) FRTIB, or (2) any employee of FRTIB in his or her official capacity, or (3) any employee of FRTIB in his or her individual capacity where DOJ or FRTIB has agreed to represent the employee, or (4) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and FRTIB determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which FRTIB collected the records.
15. Litigation, Opposing Counsel: A record from this system of records may be disclosed to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena.
16. NARA/Records Management: A record from this system of records may be disclosed to the National Archives and Records Administration (NARA) or other Federal Government agencies pursuant to the Federal Records Act.
17. Security Threat: A record from this system of records may be disclosed to Federal and foreign government intelligence or counterterrorism agencies when FRTIB reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when FRTIB reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained in paper and electronic form, including on computer databases *and cloud-based services*, all of which are *securely* stored.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by name or file number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in this system are destroyed seven years after the case is closed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: FRTIB has adopted appropriate administrative, technical, and physical controls in accordance with FRTIB's security program to protect the security, confidentiality, availability, and integrity of the information, and to ensure that records are not disclosed to or accessed by unauthorized individuals.

Paper records are stored in locked file cabinets in areas of restricted access that are locked after office hours. Electronic records are stored on computer networks and protected by assigning usernames to individuals needing access to the records and by passwords set by authorized users that must be changed periodically.

RECORD ACCESS PROCEDURES: *Individuals seeking to access records within this system must submit a request pursuant to 5 CFR Part 1630. Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual, such as Power of Attorney, in order for the representative to act on their behalf.*

CONTESTING RECORDS PROCEDURES: *See Record Access Procedures above.*

NOTIFICATION PROCEDURES: *See Record Access Procedures above.*

EXEMPTIONS CLAIMED FOR SYSTEM: Pursuant to 5 U.S.C. 552a(k)(2), records in this system of records are exempt from the requirements of subsections (c)(3); (d); (e)(1); (e)(4)(G), (H), (I); and (f) of 5 U.S.C. 552a, provided, however, that if any individual is denied any right, privilege, or benefit that he or she would otherwise be entitled to by Federal law, or for which he or she would otherwise be eligible, as a result of the maintenance of these records, such material shall be provided to the individual, except to the extent that the disclosure of the material would reveal the identity of a source who furnished information to the Government with an express promise that the identity of the source would be held in confidence.

HISTORY: *81 Fed. Reg. 7,106 (Feb. 10, 2016).*

[FR Doc. 2019-06165 Filed: 3/29/2019 8:45 am; Publication Date: 4/1/2019]